CYBERSECURITY INCIDENT RESPONSE CHECKLIST

☐ 1. Determine Current Security Posture

- Identify Cybersecurity Tools To Be Used During Remediation
- Identify "Normal Point Of Reference" To Return To After An Incident

☐ 2. Identify Key Stakeholders

- Include Members From Leadership, Information Technology, Operations Finance, Legal, Public Relations, And Others As Necessary

☐ 3. Gain Buy-In From Board Of Directors & Leadership

- An Incident Response Plan Requires Support & Cooperation From All Business Units

☐ 4. Engage Stakeholders From Business Units

- Engaging Business Unit Stakeholders Creates A More Comprehensive Plan & Increases Commitment To The Plan From Across The Organization

☐ 5. Identify Key Partners & Place On Retainer

- Utilize Outside Experts For Technology, Legal, And Public Relations Operations To Reduce Recovery Time And Increase Legal Protections

☐ 6. Document & Communicate

- Clearly Document The Incident Repose Plan

☐ 7. Test and Validate DR Plans

- Test at regular intervals at the very least annually
- Clearly Document The Incident Repose Plan

☐ 8. Test The Plan

- Test The Plan And Adjust As Necessary
- Routinely Test The Plan Once Finalized Quarterly, Semi-Annually, or Annually

☐ 9. Finalize, Print, Distribute

- All Key Stakeholders Including C-Level Leadership, Board Of Directors, and Business Units Should Have a Printed & Digital Copy Store both On And Off-Site

---

FIRST FOUR CALLS

1 ATTORNEY
BrownWinick
P: 888.282.3515

2 INSURANCE
_____
_____

3 TECHNOLOGY
ACS
P: 855.723.3628

4 PUBLIC RELATIONS
STRATEGIC AMERICA
P: 515.453.2000